УДК 657.6

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

***А.В. Бруйло**, 4 курс*
*Научный руководитель – **Н.В. Добрыдень**, преподаватель-стажер*
Полесский государственный университет

На сегодняшний день информационные технологии играют значительную роль в обеспечении эффективного выполнения бизнес-процессов субъектов хозяйствования. Повсеместное использование информационных технологий в деятельности предприятий обуславливает необходимость решать проблемы, связанные с защитой данных.

За последние годы, в Республике Беларусь, наблюдается увеличение числа атак на автоматизированные системы, которые приводят к значительным финансовым и материальным потерям.

Вот поэтому, главной целью любой системы обеспечения информационной безопасности должно быть создание необходимых условий функционирования предприятия, предотвращение угроз его безопасности, защита законных интересов предприятия от противоправных посягательств, недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечение в рамках производственной деятельности всех подразделений предприятия [1, с. 5].

Чтобы оценить состояние информационной инфраструктуры предприятия и разработать методы, с помощью которых можно было бы достичь соответствия состояния информационной инфраструктуры потребностям бизнеса, а также для достижения информационной безопасности в современном мире служит аудит информационной безопасности, понятие, сущность и этапы которого будут рассмотрены в рамках настоящей статьи.

На сегодняшний день специалистами используется несколько определений аудита информационной безопасности, но наиболее часто применяется следующее: аудит информационной безопасности – это процесс получения объективных качественных и количественных оценок текущего состояния информационной безопасности предприятия в соответствии с определенными критериями и показателями безопасности [3].

Аудит информационной безопасности должен проводиться квалифицированной аудиторской компанией, получившей аккредитацию на проведение таких проверок. Процедуры аудита информационной безопасности предполагают наличие определенного мастерства в данном вопросе для эффективного выполнения. Так, более детальные шаги аудита обычно должны разрабатываться аудитором ИС на основе конкретного программного обеспечения, а также методов и средств управления, используемых проверяемой организацией.

Аудит информационной безопасности особенно целесообразно проводить в тех случаях, когда требуется актуальная информация и независимая оценка состояния информационной безопасности. Необходимость в этом может возникнуть в следующих ситуациях:

- если предприятие меняет свою стратегию;
- при слиянии или поглощении компаний;
- когда в значительной степени изменяется организационная структура предприятия или происходит смена руководства;
- при появлении новых внутренних или внешних требований в области информационной безопасности;
- в случае значительных изменений бизнес-процессов или ИТ-инфраструктуры.

Аудит информационной безопасности проводиться в несколько этапов.

Первый этап – планирование. На данном этапе аудитор достигает понимания компьютерных операций и средств управления организации, и соответствующих рисков, а также определяет границы проведения аудита [2, с. 129].

Планирование позволяет аудитору и руководству аудиторской группы определять эффективные и продуктивные методы получения данных, необходимых для оценки компьютерных средств управления организации.

Второй этап – обследование информационной системы. На данном этапе аудитор запрашивает необходимую информацию, проводит анкетирование и интервью с работниками предприятия, осматривает помещения и многое другое. Данный этап является наиболее сложным и длительным. Это связано в основном с отсутствием необходимой документации на информационную систему и с необходимостью плотного взаимодействия аудитора со многими должностными лицами предприятия.

Третий этап – анализ данных аудита. Анализ собранной информации проводится с целью оценки текущего уровня защищённости автоматизированной системы заказчика. В процессе анализа определяются и оцениваются риски, связанные с угрозами безопасности информационных ресурсов и которым может быть подвержено предприятие. Также на данном этапе разрабатываются модели угроз информационной безопасности и в дальнейшем моделируюся действия внешнего и внутреннего нарушителя.

Заключительный этап – составление отчета аудитора и разработка рекомендаций по повышению уровня защиты автоматизированной системы от угроз информационной безопасности. Качество отчета характеризует качество работы аудитора. Отчет должен обязательно содержать описание целей проведения аудита, характеристику информационной системы заказчика, в нем должны быть указаны границы проведения, результаты анализа данных аудита, выводы и, конечно же, рекомендации аудитора по устранению существующих недостатков и совершенствованию системы защиты [2, с. 129].

Аудиторский отчет предоставляет заказчику такие возможности, как:

- обнаружить каналы утечки важной информации;
- определить меры защиты финансовых программ (1С и других);
- составить оптимальную схему резервирования данных предприятия;
- повысить уровень защиты информации и минимизировать бизнес-риски;
- и другие [4].

Необходимо отметить, что рекомендации аудитора должны быть конкретными и применимыми к данной информационной системе, экономически обоснованными и аргументированными, то есть подкрепленными результатами анализа, а также отсортированными по степени важности. Как правило, разработанные рекомендации направлены не на полное устранение всех выявленных рисков, а лишь на их уменьшение до приемлемого уровня.

Таким образом, аудит информационной безопасности – один из важнейших этапов построения надежной системы защиты информации предприятия. Проведение комплексной проверки позволяет описать полную картину состояния информационной безопасности на предприятии, и по результатам проверки устранить имеющиеся проблемы и слабые места системы защиты, и в конечном счете разработать эффективную программу построения системы информационной безопасности предприятия. Кроме того, аудит информационной безопасности не должен является однократной процедурой, а должен проводиться регулярно. Только в этом случае аудит будет приносить положительный эффект и способствовать повышению уровня информационной безопасности предприятия.

Списокиспользованных источников

1. Аверченков В.И. Аудит информационной безопасности: учеб. пособие. М.: ФЛИНТА, 2011. – 269 с.

2. Курило А.П. Аудит информационной безопасности: учеб. Пособие. М.: Издательская группа ”БДЦ-пресс“, 2006. – 304 с.

3. Словарь бизнес-терминов / Внешний аудит. 2014. – [электронный ресурс] – Режим доступа. – URL: http://dic.academic.ru/dic.nsf/business/2440 (дата обращения 12.12.2014).

4. Частная полицейская компания / Комплексный аудит информационной безопасности. 2014. – [электронный ресурс] – Режим доступа. – URL: http://policeprivat.com/kompleksnyy-audit-informacionnoy-be (дата обращения 12.12.2014).